

GENERAL INFORMATION

Company: Company Ltd.
Address: Street n.n., City, Country
URL: <http://www.company.local>
IP address: 192.168.0.4
Test start: 15th October 2006., 9:00h
Test end: 16th October 2006., 16:00h
Responsible person: John Smith, john.smith@company.local



APPLICATION INFORMATION

Platform: PHP 4.3.2
Web Server: Apache-AdvancedExtranetServer/2.0.47
Operating system: Linux Mandrake 6.12.92mdk



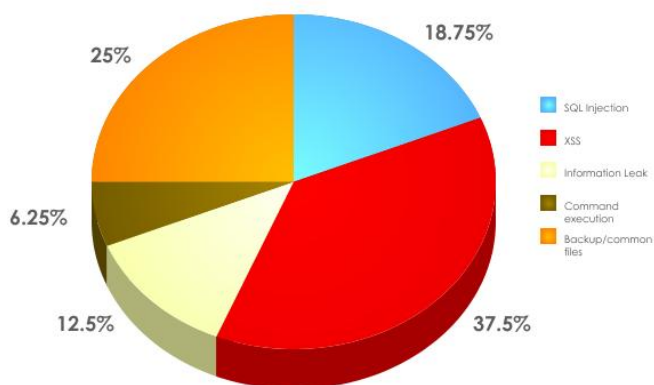
SUMMARY

1. Vulnerabilities by type

- SQL injection 3
- XSS 6
- Information leak 2
- Unauthorized file creation 0
- Command execution 1
- Backup/common files 4
- Directory traversal 0
- Misconfiguration 0

TOTAL: 16

Vulnerabilities by type

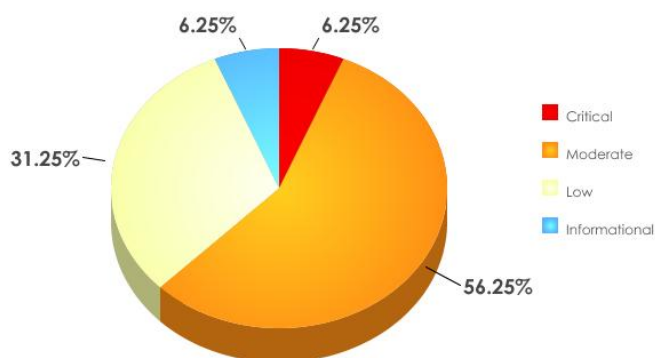


SUMMARY

2. Vulnerabilities by risk level

Critical	1
Moderate	9
Low	5
Informational	1

Vulnerabilities by risk level



OVERALL RISK ASSESSMENT

The overall risk level of the tested Web application is estimated as **VERY HIGH**.



LEGEND:



RECOMMENDATION

Security assessment of the Web application <http://www.company.local> has shown a number of vulnerabilities which may have serious impact on the overall system's security. Among other vulnerabilities, the highest risk poses a **common execution** vulnerability which enables attacker to execute system commands on the Web server. Furthermore, a number of medium risk **SQL Inject** and **XSS** vulnerabilities has also been found.

Detail evaluation of application code and strict filtering of application's input is recommended. In the particular case attention should be paid to the parameters which are used to form the SQL query or to execute system commands. Similarly, input filtering should be applied to all the characters which are displayed within the Web page, and which are controlled by the user.

Vulnerable URL example: [http://www.company.local/vuln.php?strCopyTableOK=".passthru\('cat%20/etc/passwd'\)."](http://www.company.local/vuln.php?strCopyTableOK=)